Список литературы

1. *Баумейстер Д., Экерт А., Цайлингер А.* Физика квантовой информации. – М.: «Постмаркет», 2002. – 376 с.
2. *Dusek M., Lutkenhaus N., Hendrych M.* Quantum Cryptography // Progress in Optics. – V. 49. – «Elsevier», 2006. – P. 381–454.
3. *Корченко О.Г., Василіу Є.В., Гнатюк С.О.* Сучасні квантові технології захисту інформації // Науково-технічний журнал «Захист інформації». – 2010, № 1. – С. 77–89.
4. *Cerf N.J., Bourennane M., Karlsson A., Gisin N.* Security of quantum key distribution using d-level systems // Physical Review Letters. – 2002. – V. 88, №12. – 127902.
5. *Bruss D., Macchiavello C.* Optimal eavesdropping in cryptography with three-dimensional quantum states// Physical Review Letters. – 2002. – V. 88, № 12. – 127901.
6. *Liang Y.C., Kaszlikowski D., Englert B.-G., Kwek L.C., Oh C.H.* Tomographic quantum cryptography // Physical Review A. – 2003. – V. 68, № 2. – 022324.
7. *Kaszlikowski D., Chang K., Oi D.K.L., Kwek L.C., Oh C.H.* Quantum cryptography based on qutrit Bell inequalities // Physical Review A. – 2003. – V. 67, № 1. – 012310.
8. *Ekert A.* Quantum cryptography based on Bell's theorem // Physical. Review Letters. – 1991. – V. 67, № 6. – P. 661–663.
9. *Csiszar I., Korner J.* Broadcast channels with confidential messages // IEEE Transactions on Information Theory. – 1978. – V. IT-24, № 3. – P. 339–348.

Поступила 12.01.2010

УДК 004.056 **Паціра Є.В., Захарова М.С., Корченко А.О.**

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ВПЛИВУ ТА ПОВОДЖЕННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІД ДІЄЮ КІБЕРАТАК

Інформаційні ресурси є одним з обов'язкових елементів, необхідних для здійснення будь-якого виду людської діяльності: виробництва, управління, наукових досліджень, проектування нової техніки і технології. Найважливішим аспектом взаємин споживача і інформаційної системи є по можливості якнайповніше і раціональніше забезпечення ефективного використання інформаційних ресурсів [2]. Саме ефективне використання інформаційних ресурсів таким чином дозволяє мінімізувати витрату усіх інших видів ресурсів при інформаційному забезпеченні споживачів. Тому, відповідно до існуючих підходів, прийнято вважати, що інформаційна безпека системи забезпечена у разі, якщо для будь-яких інформаційних ресурсів (ІР) в системі підтримується певний рівень конфіденційності , цілісності та доступності.

Таким чином, вирішення проблеми вибору ефективних методів забезпечення безпеки інформаційних ресурсів пов'язане з визначенням найбільш небезпечних для конкретних типів ІР класів кібератак, а також з виявленням впливу кібератак на ІР, при якому здійснюється порушення основних характеристик безпеки ресурсів.

При побудові моделі впливу кібератак на ІР необхідно, розглянути саму можливість впливу кожної кібератаки з множини $R = \{R_1, R_2, ..., R_N\}$ на кожен ІР (див. рис. 1). У результаті одержимо інтенсивності $\beta_{nm}(t)$ потоку n-ої кібератаки на m-й ІР. Потік кібератак на ІС описується розподілом імовірностей проміжків часу між сусідніми атаками. Потік кібератак R_n на ІС є ординарним - атаки з'являються поодинці, ординарність потоку атак означає, що імовірність влучення на елементарну ділянку Δt двох або більш атак мала в порівнянні з імовірністю влучення на нього рівно однієї події, тобто при $\Delta t \to 0$ ця імовірність являє собою нескінченно малу вищого порядку; потоком без наслідку - для будь-яких, що не перекриваються, ділянок часу π_1, π_2,..., π_n числа рівні кількості атак, що попадають на ці ділянки, являють собою незалежні випадкові величини, тобто імовірність влучення будь-якого числа атак на одну з ділянок не залежить від того, скільки їх потрапило на інші. Сума потоків атак

різних кібератак на будь-який ресурс буде сходитися до пуассоновского потоку, для якого справедливе твердження, що при додаванні будь-якого числа N незалежних ординарних потоків буде виходити знову ординарний потік [4], інтенсивність якого дорівнює сумі інтенсивностей потоків, що складаються. Для інформаційного ресурса X_m інтенсивність сумарного потоку усіх кібератак з множини R буде дорівнює $\beta_m(t) = \sum_{n=1}^{N} \beta_{nm}$, а для інтенсивності потоку кібератак на ІС у цілому буде справедлива рівність $\beta_m(t) = \sum_{n=1}^{N}\sum_{m=1}^{M} \beta_{nm}(t)$.

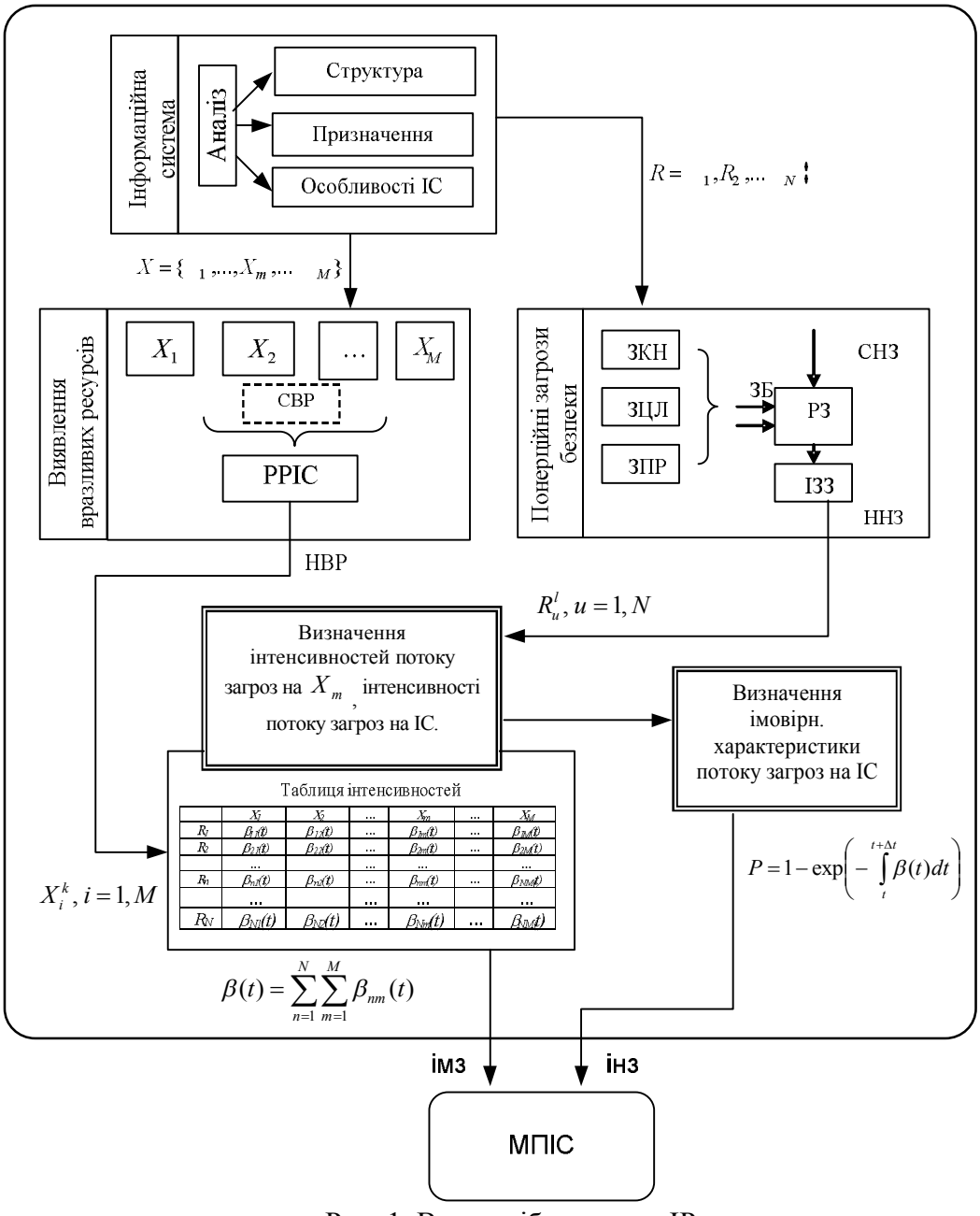

Рис. 1. Вплив кібератак на ІР

Якщо параметр β пуассоновского закону залежить від часу, тобто потік виникнення атак неоднорідний, то імовірність виникнення c атак на ділянці часу Δt описується для ресурса m і кібератаки n

$$P_{nm} = \frac{1}{c!}\left(\int_t^{t+\Delta t} \beta_{nm}(t)dt\right)^c \exp\left(-\int_t^{t+\Delta t} \beta_{nm}(t)dt\right)$$

для ресурсу m і множини кібератак $R = \{R_1, R_2, ..., R_N\}$

$$P_m = \frac{1}{c!}(\int_t^{t+\Delta t} \beta_m(t)dt)^c \exp(-\int_t^{t+\Delta t} \beta_m(t)dt)$$

для ІС і множини кібератак $R = \{R_1, R_2, ..., R_N\}$

$$P = \frac{1}{c!}(\int_t^{t+\Delta t} \beta\ (t))^c \exp(-\int_t^{t+\Delta t} \beta\ (t)dt)$$

Якщо число атак, які попадають на інтервал Δt розподілено за законом Пуассона, вважаючи c=0 та враховуючи що 0!=1, одержимо імовірність того, що за інтервал часу Δt не відбудеться ні однієї кібератаки на ІС

$$P(t, \Delta t) = \exp(-\int_t^{t+\Delta t} \beta\ (t)dt)$$

Подія, що складається в тім, що на ІС буде зроблена хоча б одна атака на інтервалі Δt, є протилежною події ненападу на ІС на тій же ділянці часу.

Тоді імовірність кібератаки на інтервалі Δt буде визначатися:

$$P(t, \Delta t) = 1 - P_0(t, \Delta t) = 1 - \exp(-\int_t^{t+\Delta t} \beta\ (t)dt)$$

Таким чином, основними етапами дослідження впливу кібератак на інформаційні ресурси є проведення аналізу ІС, виявлення найбільш вразливих ресурсів та ранжирування атак за ступенем небезпечності, а також визначення інтенсивностей та імовірнісних характеристик атак, що дозволяє побудувати модель впливу кібератак (МВКА) на ІР .

Для виявлення найбільш небезпечних класів кібератак та аналізу станів системи при впливі кібератак, проведено дослідження поводження ІС [3] при впливі кібератак (див. рис. 2). При побудові моделі поводження ІС під впливом кібератак (МПІС) (див. рис. 2) необхідно проведення аналізу можливих комбінацій кібератак, переходів ІР з стану в стан; визначення інтенсивностей переходу та проведення оцінки функціонування ІР.

Для дослідження таких процесів необхідні великі обсяги вихідних даних, що є досить трудомісткою задачею, але переважна більшість вихідних даних у даний час відсутня, тому необхідно використовувати методи експертних оцінок. Наприклад, на основі експертних досліджень за допомогою пакету Fuzzy Logic Toolbox системи MATLAB отримані оцінки ступіня небезпеки кібератак та рівня вразливості інформаційних ресурсів, на основі яких можна визначити ймовірності реалізації кібератак [5] (див. табл. 1).

Таблиця 1

Одержання оцінок ймовірностей реалізації кібератаки

Ступінь небезпеки кібератаки	Рівень вразливості ресурсу	Ймовірность реалізації кібератаки
0,79	0,87	0,754
0,44	0,37	0,374
0,53	0,41	0,419
0,22	0,01	0,195
0,48	0,64	0,5
0,6	0,764	0,599

Візуалізація результатів використання механізму нечіткого виводу здійснюється за допомогою GUI-модуля Surface Viewer (див. рис. 3).

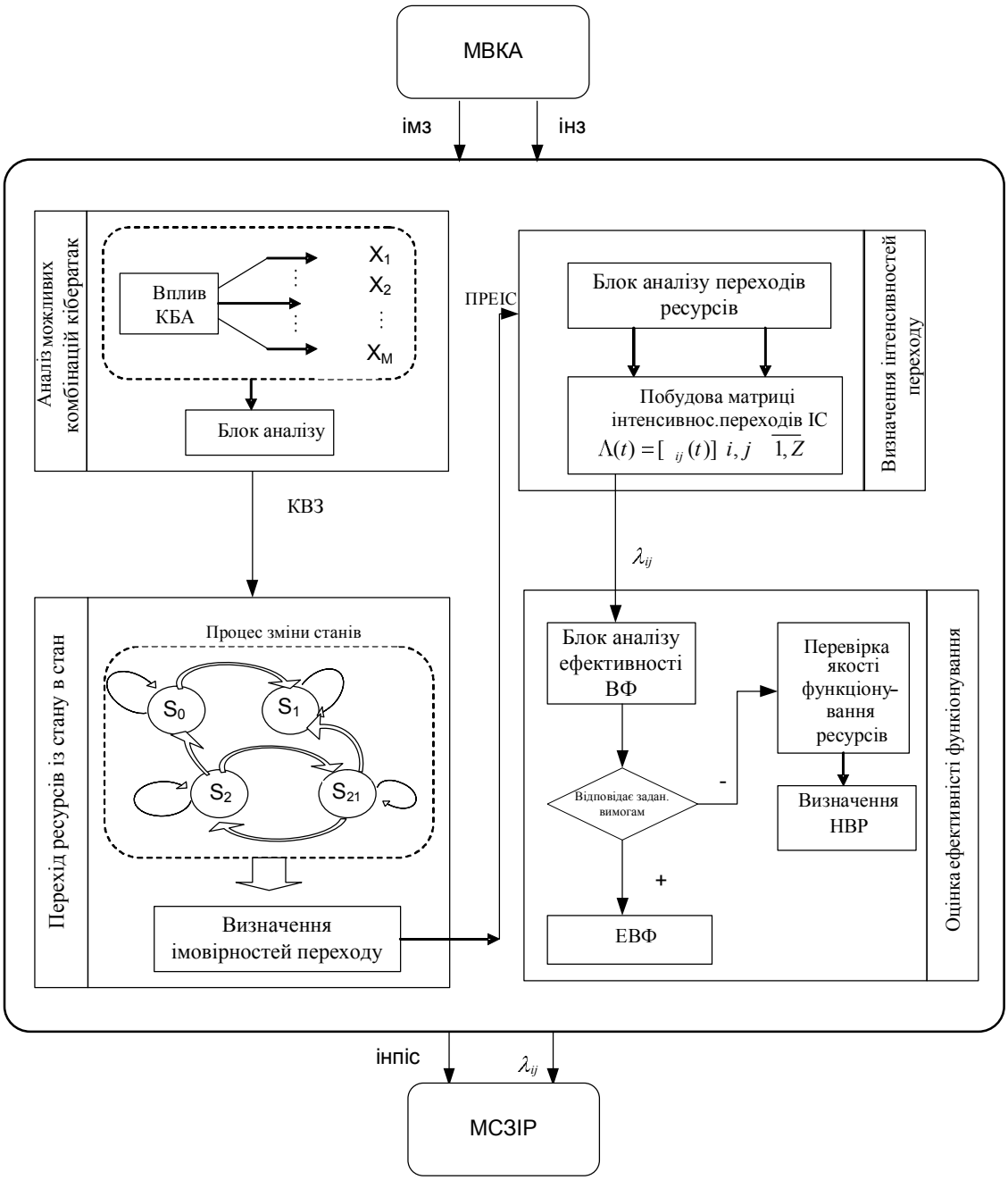

Рис. 2. Модель поводження системи при впливі кібератак

В результаті дослідження впливу кібератак на інформаційні ресурси, запропоновано модель впливу кібератак на інформаційні ресурси, яка за рахунок визначення інтенсивностей потоків кібератак на ІС дозволяє розширити множину характеристик кібератак, а також виявити найбільш вразливі інформаційні ресурси.

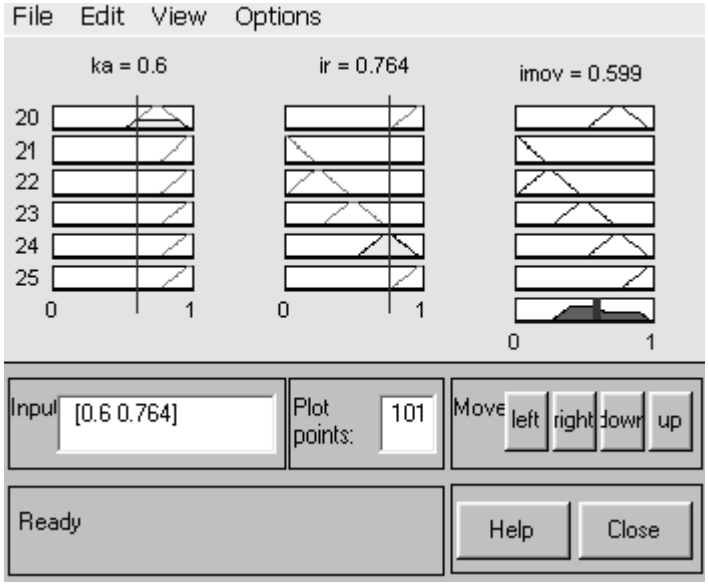

Рис. 3. Фрагмент вікна використання механізму нечіткого виводу

На основі МВКА отримала подальший розвиток модель поводження системи при впливі кібератак, що дозволяє у лінгвістичних термах виявити наслідки прояву найбільш небезпечних для конретних типів ресурсів кібератак.

Список літератури

1. *Харченко В.П., Чеботаренко Ю.Б., Корченко А.Г., Пацира Е.В., Гнатюк С.А.* Кибертерроризм на авиационном транспорте, Проблеми інформатизації та управління. Збірник наукових праць: Випуск 4(28).- К.:НАУ, 2009.

2. *Меняев М.Ф.* «Информационные технологии управления. В 3 т. Т. 2: Информационные ресурсы», Омега-Л, Учебное пособие, 2003.

3. *Захарова М.В*. Аналіз поводження інформаційної системи при впливі загроз // Тези науково-технічної конференції «Захист інформації з обмеженим доступом та автоматизація її обробки».- Київ, НАУ, 2009.

4. *Чистяков В.П*. Курс теории вероятностей. – М., Агар, 1996.

5. *Корченко А.Г., Паціра Є.В., Захарова М.В*. Оцінювання потенційного збитку інформаційних ресурсів при впливі загроз безпеки // Науково-практична конференція «Современные тренажерно-обучающие комплексы и системы –ТКС 2008», Партенит (АР Крым), 2008.

Надійшла 16.03.2010

УДК 004.056.55(045) **Корченко А.Г., Малофеев А.В., Хохлачева Ю.Е.**

КОНВЕЙЕРНЫЙ КРИПТОГРАФИЧЕСКИЙ ВЫЧИСЛИТЕЛЬ РЕАЛЬНОГО ВРЕМЕНИ

В настоящее время для надежного обеспечения конфиденциальности информации применяются криптографические алгоритмы. Использование процессоров и микроконтроллеров, позволяющих защитить информацию посредством выполнения процедур шифрования, стало одним из наиболее эффективных средств борьбы с несанкционированным доступом. Вопросы реализации в реальном времени криптографических алгоритмов остаются по-прежнему актуальными. Программное исполнение указанных алгоритмов не позволяет достичь высокой скорости шифрования. Поэтому средства защиты с такой реализацией не всегда можно использовать в системах